UNIVERSIDAD DE LA RIOJA

TRABAJO FIN DE ESTUDIOS

Título

Los delitos en Internet

Autor/es

ALEJANDRO MATA FIGUERO

Director/es

SERGIO PÉREZ GONZÁLEZ

Facultad

Facultad de Ciencias Jurídicas y Sociales

Titulación

Grado en Derecho

Departamento

DERECHO

Curso académico

2017-18

publicaciones.unirioja.es
E-mail: publicaciones@unirioja.es

UNIVERSIDAD DE LA RIOJA

TRABAJO DE FIN DE GRADO

GRADO EN DERECHO

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

CURSO ACADÉMICO 2017/2018

LOS DELITOS EN INTERNET

ALEJANDRO MATA FIGUERO

TUTOR: DR. SERGIO PÉREZ GONZÁLEZ

Resumen:

En este estudio trataremos de clarificar qué delitos del Código Penal pueden cometerse a través de Internet, y sistematizarlos, porque aunque afecten a bienes jurídicos distintos, el medio comisivo los emparenta. Realizaremos un recorrido por los antecedentes de Internet y veremos los factores que influyen en la aparición y proliferación de las conductas delictivas en la red, realizando un estudio de cada ciberdelito, siempre en el contexto del Código Penal español de 1995, sin entrar en un análisis internacional. Con ello justificaremos la necesidad de aunar todos estos delitos.

Abstract:

In this study we will try to clarify which crimes of the Penal Code can be committed through the Internet, and systematize them, because even if they affect different legal rights, the commissary media links them. We will take a tour of the Internet background and see the factors that influence the appearance and proliferation of criminal behavior in the network, conducting a study of each cybercrime, always in the context of the Spanish Criminal Code of 1995, without entering into an analysis international. With this we will justify the need to combine all these crimes.

ÍNDICE

Introducción

Internet es hoy en día la "Red de redes", un complejo y entramado sistema aparentemente invisible e intangible, pero de cuya existencia no puede dudar ni el mayor de los escépticos. A través de él se conectan millones de personas diariamente para la realización de infinitos usos, ya sean económicos, políticos, sociales, o de ocio, lo cual es posible gracias al progreso de la ciencia y la tecnología, provocando nuevas formas de entendimiento de la realidad (virtual), en la que el espacio y el tiempo han sido profundamente modificados.

Internet además de ofrecernos las mencionadas ventajas, actualmente está suponiendo un nuevo medio para la comisión de ilícitos, vulnerando bienes jurídicos como la intimidad, la propiedad intelectual y el patrimonio, la integridad, la propia imagen, o la libertad de expresión entre otros.

En este estudio trataremos de clarificar qué delitos del Código Penal pueden cometerse a través de Internet, y sistematizarlos, porque aunque afecten a bienes jurídicos distintos, el medio comisivo los emparenta.

Antes de abordar de lleno cuál es el objeto de un ciberdelito, qué tipos hay y qué medidas podemos establecer para reprimirlos, debemos estudiar el medio en el que se producen, realizando un análisis del concepto, origen y desarrollo de Internet para comprender su funcionamiento como un verdadero medio de comunicación. Explicaremos los problemas que rodean su persecución e identificación, y posteriormente definiremos el ciberdelito, dividiendo los principales por capítulos referentes a los delitos contra la intimidad, libertad, honor y patrimonio y orden socioeconómico.

Con todo, trataremos finalmente de justificar la necesidad de aglutinar todas las conductas maliciosas y delictivas que pueden cometerse a través de Internet, logrando unidad de criterios, actuaciones, y consiguiendo así mayor seguridad en el tránsito de los usuarios por la red.

BLOQUE 1º

Capítulo 1.- La creación y el desarrollo de Internet

Para conocer el origen de Internet debemos remontarnos a mediados de los años sesenta, cuando el empleo de redes de comunicación manejadas por computadoras adquirió nuevos visos de aplicación en actividades estratégicas. Este fue el objetivo del Departamento de Defensa de Estados Unidos al diseñar una red de comunicación entre sus miembros.

La gestión de esta red de subredes por el Departamento de Defensa se llevó a cabo a través de la Agencia para Proyectos de Investigación Avanzada, conocida como DARPA (Defense Advanced Research Projects Agency). La fecha oficial fue 1969, si bien su primera demostración oficial no se dio hasta 1972[1].

Con el paso de los años y el avance de la tecnología, se fueron cambiando e introduciendo nuevos protocolos, y ampliando el radio de comunicación posible hasta la creación del primer navegador web y los motores de búsqueda, trayendo consigo el surgimiento de un nuevo perfil de usuarios, en su mayoría de personas comunes no ligadas a los sectores académicos, científicos y gubernamentales.

Hoy, el índice de crecimiento de internet no tiene precedentes, está transformando sectores económicos tradicionales, creando nuevos mercados, reduciendo los costes y mejorando el servicio al cliente. Se están creando nuevas oportunidades para las pequeñas y medianas empresas a través de lo que se conoce como el servicio de World Wide Web[2].

Desde su creación, y continuo perfeccionamiento Internet ha venido proporcionando unos innegables beneficios a nivel global, permitiendo una comunicación permanente entre usuarios ubicados en diferentes sitios geográficos a un bajo costo; posibilita compartir y divulgar información a gran escala, permite a las empresas promocionar sus productos; fomenta la ciencia y la tecnología, y es fuente de conocimiento e información; ha creado un comercio Internacional mejorando las condiciones y servicios, permitiendo realizar transacciones bancarias que de otro modo tardarían días o incluso semanas...Internet, en suma, ha mejorado nuestro mundo.

Desde este punto de vista, los beneficios de Internet son incuestionables, y su contribución al desarrollo de la Sociedad de la Información, debe promoverse y protegerse. Internet canaliza los derechos clásicos, como la libertad de expresión, la diversidad cultural, el pluralismo ideológico, el desarrollo de la persona, etc. Por ello, como afirma Velasco Núñez[3], "el único límite a la realidad virtual se encuentra, como en la realidad real, valga la redundancia, en la protección del interés público, y esa es la razón por la que se dice que lo que es ilícito fuera de la Red, debe también serlo dentro de la misma".

---

[1] Briggs y Burke: *De Gutenberg a Internet, una historia social de los medios de comunicación*. Madrid, Santillana Ediciones Generales, S. L., 2002 .Pg. 345.

[2] Morón Lerma: *Internet y derecho penal: Hacking y otras conductas ilícitas en la Red*. Editorial Aranzadi, 2ª Edición. Pg. 113.

[3] Velasco Núñez: "Eliminación de contenidos ilícitos y clausura de páginas web en Internet (medidas de restricción de servicios)". *Cuadernos de derecho judicial*, 2007, tomo 3. Pg. 7

Capítulo 2.- Necesidad de un Régimen Jurídico propio para Internet

Como afirma Terceiro[4], "la humanidad ha venido midiendo su progreso históricamente en términos de tecnología, y en nuestra era, la tecnología más importante (revolucionaria) es Internet, si bien el sustrato de la misma es la información, entendiendo ésta como un recurso autónomo, generador de riqueza y de poder". Debemos entender la información como un valor económico en sí misma, como un bien que no se agota con su consumo, como un servicio, que consta con un régimen económico y jurídico propio.

La información nace en gran parte de la comunicación; en el ciberespacio cada individuo es potencialmente un emisor y un receptor en un medio cualitativamente diferenciado, en el que todos comunican con todos, un mundo virtual segregado por la comunicación. "El mundo digital es el mundo de la información convertida en dígitos, y el mundo analógico es todo lo demás"[5].

Digitalizar significa convertir en números lo que se quiere transmitir; la digitalización permite que distintos tipos de datos y de información, como textos, voz e imágenes puedan convertirse en números, ser tratados del mismo modo y transmitidos por las mismas líneas.

Las conductas maliciosas y delictivas realizadas a través de Internet se han expandido debido a la absoluta digitalización[6] de nuestra vida diaria, tanto desde una perspectiva local como personal; como veremos más adelante, el anonimato que otorga la red, la facilidad con que pueden cometerse (y ocultarse) estos ilícitos, y las dificultades de persecución y prueba que los caracteriza, con respuestas normalmente tardías por carencias competenciales de los tribunales debido a la trasnacionalidad de las conductas, sitúan al delincuente en una situación de superioridad respecto de la víctima (incluso antes de cometer el delito), impidiendo a esta defenderse ni siquiera por los cauces legales en muchas ocasiones.

Por lo tanto, Internet permite la plasmación de una realidad física en un mundo virtual a través de la digitalización, convirtiendo hechos, obras, acontecimientos y noticias en datos, y por tanto en información. La pregunta que debemos hacernos llegados a este punto es si Internet puede configurarse como un escenario paralelo al mundo físico, y por tanto aplicar las mismas normas, o bien considerarlo como un plano autónomo de la realidad en la que vivimos, debiendo así crear un nuevo corpus normativo para las conductas que se realicen a través de él, considerando, por tanto, que protegemos bienes jurídicos nuevos.

Trasladado esto al derecho penal, debemos analizar si hay un delito específico de Internet o, si por el contrario, estamos ante delitos clásicos y tipificados como tales en los ordenamientos que se singularizan por el específico lugar de comisión cibernética.

---

[4] Terceiro: *Socied@d Digital. Del homo sapiens al homo digitalis*. Madrid, Alianza Editorial. 1996. Pg. 29.
[5] Morón Lerma: *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la Red*. Aranzadi, 2002 pg. 96
[6] De la Mata Barranco: "Ilícitos vinculados al ámbito informático: la respuesta penal" en *Derecho penal Informático* (parte I, capítulo I). Pamplona, Civitas, 2010. Pg. 17.

Y en relación con lo expuesto, también hemos de analizar si la Red se configura como un verdadero "lugar", a pesar de no existir coordenadas espacio-temporales, un espacio virtual, un "ciberespacio"[7], en el que puedan converger los elementos necesarios para la consumación de un delito, o la puesta en peligro de un determinado bien jurídico.

Si atendemos a criterios fácticos y objetivos, Internet se equipara al mundo físico en las conductas que a través del mismo pueden realizarse; en la realidad física es posible robar un objeto, revelar un secreto, mirar dentro de una carpeta que ponga Top Secret, divulgar fotografías ajenas, utilizar llaves falsas y claves de palabra que hayamos obtenido ilícitamente. En Internet todo lo descrito puede realizarse virtualmente, podremos utilizar claves de acceso obtenidas mediante programas, revelar secretos íntimos o empresariales a través de redes sociales, donde igualmente podremos divulgar fotografías ajenas, así como introducirnos en las cuentas bancarias de otra persona y realizar traspasos de capitales, con un mayor peligro, pues todas las conductas definidas no necesitan de contacto directo, sino que pueden realizarse a kilómetros de distancia, presentando mayores problemáticas de perseguibilidad que más adelante analizaremos.

De este modo, puede afirmarse que Internet se constituye como una auténtica realidad virtual, como un verdadero espacio en el que simplemente introducimos el elemento novedoso del ordenador, de la Red, debiendo así analizar cómo debe ajustarse la protección de los bienes jurídicos tradicionales al nuevo medio empleado de la informática, siendo así una nueva faceta de una sociedad descentralizada, pues no existe una sede central ni un presidente, pero como ya dijo Tomás de Aquino, "ubi societas, ibi ius"[8], es decir, "donde hay sociedad, hay derecho", o en este caso, debe haberlo.

Encontramos, así en un primer acercamiento uno de los motivos más esenciales para la creación de un Régimen Jurídico para Internet, para regular el conjunto de intercambios y conductas que se realizan a través de la red, pues en nuestra era, no podemos permitir que ningún aspecto de la sociedad, escape al control de la legalidad, debiendo quedar los derechos de los ciudadanos debidamente garantizados y protegidos.

[7] De la cuesta Arzamendi: "La cibercriminalidad: interés y necesidad de estudio, percepción de seguridad e inseguridad", en *Derecho penal Informático* (parte II, capítulo I). Pamplona, Civitas, 2010. Pg. 57 y ss.
[8] García Mexía: *Principios de derecho en Internet*. 2ª Edición, Tirant lo Blanch, 2005. Pag. 109.

Capítulo 3.- Dificultad de persecución de los delitos a través de Internet

3.1.-Ámbito espacial y temporal

Dada la trasnacionalidad de los comportamientos realizados a través de Internet, se puede efectuar una compra a miles de kilómetros de distancia utilizando un smartphone, igualmente, se puede estafar a distancia, o volcar contenidos pornográficos en la red ocultando el delincuente su dirección IP [9]. Estas conductas son posibles en cualquier momento y lugar, debido a la existencia de medios o aparatos de libre acceso a proveedores del servicio de Internet mediante wifi[10] o en lugares públicos como universidades, cafés, plazas o incluso supermercados, y desde cualquier dispositivo con conexión a Internet, lo cual si lo unimos al anonimato hacen que la determinación del culpable sea en muchos casos, imposible.

Esta posibilidad de delinquir a distancia, rompiendo las barreras geográficas de los Estados, genera problemas tanto de jurisdicción competente[11] -dificultando la ley aplicable, y el conocimiento cierto de la prescripción, y por tanto de persecución del delincuente- como de mecanismos para el resarcimiento de la víctima. El artículo 22 del Convenio sobre Cibercriminalidad del Consejo de Europa del 2001[12] afronta esta cuestión acudiendo al principio de territorialidad según el cual, "las partes adoptaran las medidas necesarias para atribuirse la competencia respecto de cualquier infracción penal cuando esta se haya cometido en su territorio a bordo de buque o aeronave, o por uno de los súbditos de dicho estado".

No obstante, dicha trasnacionalidad, unida a la complejidad de internet dificultan la aplicación del citado principio de territorialidad, por lo que los Estados han buscado ampliar el criterio del Convenio creando 3 teorías nuevas[13] .

Podríamos aplicar el principio de jurisdicción universal del artículo 23.4 de la LOPJ, pero ni este ni el Convenio sobre Ciberdelincuencia prevén la aplicación de este principio a los supuestos de cibercriminalidad. Por otra parte, una mala aplicación de la teoría de la acción y el resultado puede abrir la puerta para que cualquier Estado invoque su jurisdicción para el conocimiento de cualquier hecho, simplemente considerando que se ha producido un peligro in abstracto que un bien que le corresponde tutelar. Por lo que parece más razonable aplicar la Teoría de la ubicuidad: por la que se puede entender cometido el delito en el lugar de la acción, o en el lugar del resultado, indistintamente, de modo que la jurisdicción nacional entraría a conocer tanto si

[9] Fernández de Teruelo: *Cibercrimen, los delitos cometidos a través de Internet*. Constitutio Criminalis Carolina, 2007. Pg. 14.
[10] De la cuesta Arzamendi: "Aproximaciones criminológicas a la realidad de los ciberdelitos,", en *Derecho penal Informático* (Parte II, capítulo II). Pamplona, Civitas, 2010. Pg. 91.
[11] Climent Barberá: "La justicia penal en Internet. Territorialidad y competencias penales". *Cuadernos de derecho judicial*, nº10, 2001. Pgs. 657 y ss.
[12] Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. BOE-A-2010-14221. Art. 22.
[13] Pérez Machío: "Dos problemas particulares de cara a la persecución de delitos informáticos,", en *Derecho penal Informático* (parte III, capítulo V). Pamplona, Civitas, 2010. Pgs. 248-252.

la acción se llevó en su territorio y el resultado tuvo lugar fuera, como si el hecho se realizó fuera, produciéndose el resultado en su territorio

En definitiva, la realidad espacio-temporal inherente a los supuestos de ciberdelitos implica un nuevo incremento de las dificultades y obstáculos existentes para la averiguación e investigación y, en última instancia, sanción de estos comportamientos[14].

3.2.-Individualización de la Responsabilidad Penal:

Según Velasco Núñez[15], Los contenidos de Internet son "ilícitos" cuando constituyen delito en sí mismos (pornografía infantil), siendo merecedores de sanción penal, o contrarios a los derechos fundamentales. Por otra parte, los contenidos "nocivos" son aquellos que, sin alcanzar la entidad de ilícitos, son susceptibles de irrogar daño a sus destinatarios, en relación con sus convicciones éticas, religiosas o políticas, mereciendo un tratamiento tuitivo (fotografías que hieren la sensibilidad).

No siempre va a ser fácil diferenciar entre contenidos ilícitos y nocivos, pues habrá supuestos de colisión entre la protección de la libertad de expresión, y la defensa del interés público, surgiendo así cuestiones transfronterizas (como veremos en el capítulo 2).

Nos reafirmamos en que Internet presenta una estructura compleja, dentro de la cual existe una suerte de jerarquía, a la cual acudimos para determinar la individualización de la responsabilidad penal por contenidos ilícitos en la Red.

Por un lado, encontramos a los "proveedores de contenidos", que crean, producen y ponen a disposición de los usuarios los contenidos que se difunden en la Red. Por otro, los "intermediarios técnicos", también llamados ISPs, proporcionan la estructura a través de la cual se trasmite la información (proveen el acceso a Internet, motores de búsqueda, cuentas de correo electrónico o alojamiento de páginas web). Por último, los "usuarios de Internet" son los susceptibles de ser expuestos a los contenidos.[16]

Si comparamos la estructura con un inmueble arrendado, el Intermediario Técnico sería el nudo propietario, el Proveedor de contenido el arrendatario que vende droga en el piso (sin que lo sepa el proveedor de contenido), y el usuario la persona que acude a comprar droga.

En este caso el Proveedor no conoce las actividades que realiza en el inmueble la persona a quien lo tiene alquilado, por lo que no cabría aplicarle responsabilidad por la venta de la droga, y el usuario simplemente acude para comprar lo justo para consumir, por lo que únicamente debería aplicarse la responsabilidad al proveedor de contenido, pues es quien crea, introduce y difunde la droga, o los contenidos ilícitos en la Red.

[14]De la cuesta Arzamendi: "Aproximaciones criminológicas a la realidad de los ciberdelitos,", en *Derecho penal Informático* (Parte II, capítulo II). Pamplona, Civitas, 2010. Pg. 96

[15] Realiza esta diferenciación Velasco Núñez, en "Medidas restrictivas en Internet: cómo retirar contenidos ilícitos". *Cuadernos digitales de formación*. nº52, 2008. Pg. 2

[16] Velasco Núñez, op cit pg.5-6

Igualmente podríamos identificar al Intermediario con el dueño de una librería, que no conoce el contenido de todos los libros que posee. Hacemos así referencia a la responsabilidad por hechos propios o ajenos[17].

No cabe duda, por tanto, que la responsabilidad principal por los contenidos ilícitos recaerá sobre el "proveedor de contenidos", siendo así el problema jurídico principal, analizar la responsabilidad de los "intermediarios técnicos", los cuales en principio se exonerarían, pudiendo resultar penalmente responsables cuando intervienen seleccionando contenidos, los coproducen, los alientan o los conocen y no los eliminan pese a ser requeridos para ello.

Por último, debido al carácter internacional y global de estos servicios, autores y proveedores de contenido que alojan en sus páginas webs o sites contenidos ilícitos en la mayoría de países, ubican sus servidores en lugares con legislaciones más laxas y menos restrictivas[18], donde esos contenidos no son considerados ilícitos, generándose así una suerte de "paraísos para los delitos informáticos"[19], o "dumping informático".

Este es otro motivo por el que, a mi juicio, es necesario un nuevo régimen jurídico para los delitos cometidos mediante Internet, a fin de respetar el derecho de libertad de expresión, pues la otra solución sería el rastreo de contenidos en la Red, pudiendo llegar incluso a supuestos de censura previa.

3.3.- El anonimato y la encriptación

El artículo 18 de nuestra Constitución garantiza el derecho fundamental a la intimidad, la propia imagen y el secreto de las comunicaciones, y dice expresamente "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". En el plano físico las intromisiones a la intimidad ajena son evidentes, pues se garantiza un ámbito o esfera reservada a una persona, espacio que ésta puede dar a conocer en mayor o menor medida a su antojo; pero cuando nos encontramos en Internet, ningún sentido tiene reconocer el derecho al control sobre los datos personales, si estos datos ya no circulan por redes cerradas sobre las que imponer un estricto control[20]. Si nos adentramos en Internet, este derecho a la intimidad se ve superado, por lo que se creó "el anonimato", entendido como un derecho a no ser reconocido cuando transita por la red el usuario de Internet, el ciudadano electrónico[21], protegiendo el conocimiento que los otros pueden tener de los sitios consultados y visitados.

---

[17] De la Mata Barranco: "Ilícitos vinculados al ámbito informático: la respuesta penal,", en *Derecho penal Informático* (parte I, capítulo I). Pamplona, Civitas, 2010. Pg. 27.

[18] Morón Lerma: *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la Red*. Aranzadi, 2002 Pg. 128.

[19] Utiliza esta expresión Galán Muñóz, en *El fraude y la estada en los sistemas informáticos*. Valencia. Tirant lo Blanch. 2005. Pg. 42

[20] Buenaventura Ferrer Pujol. "Las nuevas tecnologías: injerencias en el ámbito de la privacidad. Su persecución penal". *Cuadernos digitales de formación*, nº43, 2010. Pg. 7

[21] Moron Lerma, op cit. Pg.142.

La Encriptación por su parte, consiste en el "cifrado de los mensajes transmitidos, tendente a incrementar el nivel de seguridad de la transmisión, aumentar el secreto y la confidencialidad de la misma, pudiendo decirse que la encriptación es un complemento del anonimato"[22].

Pero no siempre, pues encriptar algo no necesariamente requiere de la interposición de programas, mecanismos y trampas de lo más complejo, a veces simplemente consiste en una contraseña[23] para una carpeta de archivos, un perfil de correo o cuenta en una web, pues dado que en Internet todo lo que no esté cifrado será público, es a través de la encriptación a nivel primario como se protege la esfera privada de los usuarios, de modo que una mera intrusión ya será penalmente reprochable, pues el delincuente habrá que tenido que "forzar" la entrada vulnerando la contraseña.

Por otra parte, Miró Linares opina que el anonimato otorga al infractor una seguridad, al ofrecerle un refugio y adoptar nuevos personajes virtuales con los que, quizás, cometer delitos, siendo así un "agresor motivado"[24]. Si unimos el anonimato y la encriptación con la trasnacionalidad de los delitos, desaparece por completo el miedo del delincuente a ser identificado y por consiguiente a ser detenido, pues haría un balance entre los pocos riesgos que corre, los grandes beneficios que obtendría con la agresión, y la enorme dificultad que plantea hoy en día la identificación y prueba del cibercriminal.

3.4.-Ataques a personas jurídicas:

Los ataques informáticos y los distintos delitos que pueden cometerse a través de Internet presentan un elevado porcentaje de actuación en relación con personas jurídicas, pues el beneficio que puede obtener el infractor es mayor. Estos supuestos presentan una ventaja para los ciberdelincuentes, y es la actitud poco favorable a la denuncia por parte de la persona jurídica, normalmente una empresa importante, por temor de ésta a que se traduzca en una suerte de descrédito de la fiabilidad de la gestión de la propia empresa y su prestigio (lo cual sería motivo de una pérdida de confianza en los sistemas de seguridad de redes y de comunicación). Imaginemos que la empresa atacada es el Banco Santander, ¿qué opinarían sus clientes que operan diariamente por la banca online? ¿seguirían operando o se cambiarían de banco? Así, a fin de evitar mayores pérdidas, las personas jurídicas prefieren resolver estos problemas internamente, de ahí que en este tipo de delitos, el mejor cómplice del delincuente sea su propia víctima.

[22] García Mexía: *Principios de derecho en Internet*. 2ª Edición, Tirant lo Blanch, 2005. Pg. 207
[23] Urbano Castrillo: *Revelación informática de secretos y daños informáticos*. Cuadernos digitales de formación, nº22, 2009. Pg. 35.
[24] Miró Llinares: "La oportunidad criminal en el ciberespacio". *Revista Electrónica de Ciencia Penal y Criminología* 2011. Pg. 25.

3.5.- Ausencia del "Guardián Capaz"[25]

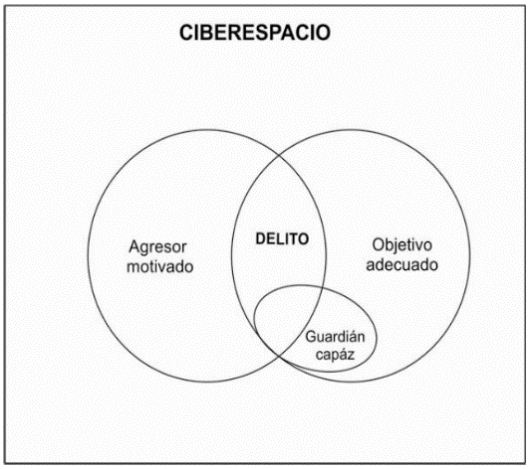
La ausencia de mecanismos centrales de protección de los servicios de Internet, y de mecanismos de control supranacional por encima de las legislaciones estatales, conlleva a la inexistencia de unos "gestores centralizados" que vigilen el ciberespacio de forma global y protejan a las potenciales víctimas. Ciertamente hay policía en Internet, pero su ámbito de actuación es muy reducido debido a la propia extensión y complejidad de la Red.

Uno de los problemas de los ciber delitos, en concreto en su variante de delitos contra la intimidad, delitos informáticos y delitos contra la propiedad intelectual, es que se pueden cometer fácilmente ya que los usuarios de la Red no presentan una clara concienciación y una buena formación acerca de los usos en internet y de qué tipo de medidas tienen que poner por medio para evitar estas conductas peligrosas. "Antivirus, cortafuegos, bloqueo de páginas, sistemas anti spam, sandbox, escudos de ransonware, escudos web cam o de datos privados, antiTrack, contraseñas para carpetas", son entre otras las medidas que pueden adoptarse a nivel particular en cada ordenador privado para evitar que los troyanos, los virus, y los crackers accedan a nuestros archivos.

Como señala Miró Llinares, "al igual que los sistemas de seguridad físicos, tales como alarmas o cerrojos especiales se han mostrado eficaces frente a la delincuencia, también pueden serlo aquellos otros que ejercen la misma función en la Red, como los antivirus o cualesquiera otros sistemas de seguridad"[26].

El Guardián Capaz hace referencia así, al conjunto de sistemas de protección y prevención contra amenazas de la red, si bien no autónomo, pues dependen de la propia víctima; en el ciberespacio es el usuario quien deberá obtener el antivirus, instalarlo, y actualizarlo periódicamente así como realizar análisis y adquirir otros software.

Como vemos en la imagen, el guardián capaz depende del propio objetivo, del usuario, pues apenas hay guardianes externos, por lo que el efecto reductor del delito es menor.



[25] Miró Llinares: "La oportunidad criminal en el ciberespacio". *Revista Electrónica de Ciencia Penal y Criminología* 2011. Pgs. 34-37.
[26] Miró Llinares. Op cit. Pg. 35

Bloque 2º

Capítulo 4.- El ciberdelito

4.1.- Definición de Ciberdelito

Al igual que el término ciberseguridad, no existe una definición singular y universalmente aceptada de ciberdelito. En algunos países se habla de delitos informáticos, en otros de ciberdelitos o cibercrimen, o simple y llanamente de delitos cometidos a través de sistemas de cómputo e internet (computer crime), sin embargo, en la mayoría de los países de habla hispana se utilizad con mayor frecuencia el término "delitos informáticos"[27].

Es necesario aquí distinguir los delitos relacionados con la informática, en tanto esta (Internet) es un medio para la realización de los mismos, de los delitos en los que la informática es el objeto del delito o la infracción[28]. Por su parte, los delitos cometidos mediante Internet consisten en la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático.

A modo de ejemplo, un delito informático serían las conductas de intrusismo informático; mientras que nos encontraríamos ante delitos cometidos mediante internet en los casos de estafas, hurtos y amenazas.

Para Davaria (2001), el delito informático consiste en "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevado a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un hardware o software"[29].

Según Velasco Núñez, se incluyen en el concepto de delito informático tanto el tradicional cometido través de ordenador o Internet (injurias a través del correo electrónico, venta de droga, extorsión y amenazas vehiculizadas a través de internet), como el propiamente tal, delito contra la informática (bloqueando sistemas, destruyendo programas, dañando dispositivos remotamente u usándolos ilícitamente como la piratería). Junto con este concepto instrumental, se acuña el de delitos telemáticos, tratando de agrupar aquellos delitos que parte o en todo se cometen a través de las nuevas tecnologías[30]. Se habla así, de que "el cibercrimen es la transformación de la delincuencia en medios informáticos o electrónicos"[31].

---

[27] Velasco San Martín: *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet*. Valencia. Editorial Titanti lo Blanch. 2012. Pg. 50

[28] Hernández Díaz: "Aproximación a un concepto de derecho penal informático" en *Derecho penal Informático* (Parte I, capítulo II). Pamplona, Civitas, 2010. De la Cuesta Arzamendi. Pg.49.

[29] García Mexía, Op. Cit. Pg. 301.

[30] Velasco Núñez: *Delitos cometidos a través de Internet, cuestiones procesales*. Madrid, Editorial La Ley, grupo Wolters Kluwer S.A. 2010. Pg. 41.

[31] Barroso Toledo: "Los delitos en Internet: Un enfoque desde la pornografía infantil en la red". *Revista F@ro*, Nº 13, 2011. Facultad de Ciencias Sociales, Universidad de Playa Ancha, Valparaíso, Chile. Pg. 2

4.2.- Clasificación delictual por "digitalización"

Dada la ilimitada extensión de la red, para realizar un análisis de los delitos que puedan cometerse a través de Internet, utilizaremos el criterio de la digitalización, entendiendo esta como el único método a través del cual pueden cometerse verdaderos delitos en la red que afecten a bienes jurídicos tradicionales. Así, realizaremos una clasificación sistemática basándonos en la tipificación del Código Penal de conductas susceptibles de realizarse on-line, tales como el hacking, interceptación de comunicaciones, cracking, sexting, child grooming entre otros. En definitiva, analizaremos cuatro bloques de delitos, empezando por aquellos que lesionan la intimidad, continuando por los delitos contra el honor, y aquellos que vulneran la libertad, y terminando con los delitos contra el patrimonio y orden socioeconómico.

Capítulo 5.- Delitos contra la Intimidad de las personas

Es necesario diferenciar intimidad de privacidad, pues si bien ambos términos están semánticamente muy próximos, privacidad no es sinónimo de intimidad. En el derecho anglosajón se conoce la privacidad como "The Right to Privacy", el derecho a la privacidad, o el "Right to be let alone", el derecho a ser dejado en paz[32]. En España, la RAE define privacidad[33] como el "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión"; del mismo modo, define intimidad[34] como la "zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia".

La intimidad y la privacidad pueden manifestarse de diversas formas, unas veces centrándose en la expresión personal que el individuo realiza de su propia vida privada, apareciendo así el descubrimiento y revelación de secretos, o la interceptación de comunicaciones. En otros casos la intimidad aparece plasmada como confidencialidad, como aquellos datos reservados que se ponen a disposición de terceros con consentimiento, quienes tienen obligación de guardar secreto[35].

El Código Penal, en su título X incluye dentro de los delitos contra la intimidad, los delitos relativos al descubrimiento y revelación de secretos en el art 197.

> "1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses."

[32] Buenaventura: "Las nuevas tecnologías: injerencias en el ámbito de la privacidad. Su persecución penal". *Cuadernos digitales de formación*, Nº 43. 2010. Pg.3.
[33] Privacidad. (2017). En: Diccionario de la Lengua Española, 23rd ed. [online] Madrid.
[34] Intimidad (2017) DEL op cit.
[35] Buenaventura, Op Cit. Pg. 6.

El precepto fija el bien jurídico de manera compleja, pues incluye los delitos que a continuación vamos a describir dentro de las vulneraciones de la intimidad, pero entiende que esta se produce con el fin de descubrir, y en un siguiente estadio revelar, un secreto, es decir, un dato reservado. Por tanto, en lo relativo a este tipo penal, el bien jurídico protegido va a ser la seguridad de las comunicaciones y los sistemas informáticos, pues entiende el legislador que es el elemento que se vulnera necesariamente para la obtención de dichos datos, y lo incluye en el título X, pues a consecuencia de lo descrito la intimidad se ve perturbada.

El precepto igualmente tipifica y penaliza conductas de apoderamiento, modificación, cesión a terceros y difusión de esos datos reservados, sin embargo, en ningún momento define o especifica qué debe entenderse por dato reservado. El "habeas data"[36], es el conjunto de derechos que constituyen la identidad informática, el derecho que tiene el titular de los datos que deben cederse a un tercero de controlar a quién los cede, a oponerse y a conocer el uso que se da de los mismos. La importancia de dichos datos podría variar en función de la persona encuestada, pues para unos será relevante su creencia religiosa, para otra su orientación sexual, y para otra su fecha de nacimiento y apellidos. Por parte de la legislación, ni la LORTAD ni la LOPD ni el Convenio del Consejo de Europa hacen una definición precisa de datos reservados, por lo que en principio todo dato personal es, objeto de protección por la norma penal, si cumple las exigencias de estar registrados en soportes informáticos, electrónicos o telemáticos.

El propio artículo 197 establece una serie de supuestos cualificados, tales como la divulgación; la condición del sujeto activo de estar encargado de los ficheros o soportes informáticos; la relevancia de los datos (que revelen información sobre ideología, religión, salud o sexo); que los hechos se realicen con fines lucrativos; o por el estatus de autoridad o funcionario público.

En su apartado séptimo, el artículo versa sobre el delito de sexting, del cual trataremos en lo relativo a los delitos contra la libertad.

5.1.- Intrusismo Informático, "Hacking"

Por otra parte, el art. 197 bis, en su apartado 1º regula un supuesto cada vez más frecuente en la actualidad, que fue introducido con la reforma del código en 2015, hablamos del "intrusismo informático" o "Hacking".

> "El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años."

Según González Rus[37], el Hacking puede definirse como "el acceso no autorizado a sistemas informáticos ajenos utilizando redes públicas de telefonía o transmisión de datos", y nombra al hacker como un individuo que tiene un elevado dominio de los mecanismos informáticos, lo cual le permite obtener dichos accesos no autorizados a sistemas informáticos ajenos, superando las

[36] García Mexía: *Principios de derecho en Internet*. 2ª Edición, Tirant lo Blanch, 2005. Pg. 308.

[37] González Rus: *Los ilícitos en la red: Hackers, Crackers, Cyberpunks, Sniffers, denegación de servicio y otros comportamientos semejantes*. En *El Cibercrimen: Nuevos retos jurídico-penales, nuevas respuestas político criminales*. Romeo Casabona (Coordinador) Ed. Comares, Granada. Pgs. 241-271)

barreras de seguridad instalados para impedirlos. Si bien los hackers no son dañinos por naturaleza, pues en muchas ocasiones se trata de jóvenes que hackean páginas webs del gobierno o determinadas entidades para hacer alarde de su habilidad, es decir, entran y vulneran las contraseñas impuestas, aunque si bien consiguen acceder a esos datos reservados, no los modifican, ni divulgan, ni causan daños, a diferencia de los Crackers o Cyberpunk, de los cuales trataremos en el apartado relativo a delitos contra el patrimonio en su vertiente de daños.

Téngase en cuenta que el precepto dice "el que por cualquier medio acceda o facilite a tercero", por lo que la conducta punible es el apoderamiento o interceptación, sin autorización, de información ajena, sin que sea necesario la revelación, o incluso sin que se llegue a conocer la información secreta, bastando así con la mera interceptación, dando sentido al concepto de mero intrusismo.

El mero intrusismo del art. 197 bis se trata por tanto de un delito de peligro, no siendo necesario un resultado más allá de la vulneración de los sistemas informáticos, accediendo a información comprometida.

Por último, el delito es necesariamente doloso[38], pero no requiere necesariamente de ánimo de lucro (pues es un caso de delito cualificado expresamente), ha de hacerse con la finalidad de descubrir los secretos de otro, siendo esto el propio elemento subjetivo del injusto, debe haber por tanto un dolo directo de vulnerar la intimidad ajena.

5.2.- Interceptación de comunicaciones

Por otra parte, el artículo 197.bis.2º tipifica la interceptación de comunicaciones, Ésta es una figura creada ex-novo tras la modificación del CP en el año 2015. El legislador ha querido criminalizar la interceptación de transmisiones no públicas de datos informáticos, así establece:

> "El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses".

En cuanto al bien jurídico protegido, tanto el hacking como la intervención de comunicaciones pese a estar incluidos en el título de delitos contra la intimidad, el artículo 197 bis trata de proteger más bien la seguridad de los sistemas informáticos[39], asemejando la vulneración de las claves de acceso a una violencia física que se ejerce para entrar en un lugar cerrado, un acceso violento a un lugar a la intimidad, lo cual aumenta las posibilidades de que el delincuente pase al siguiente estadio, al apoderamiento de dichos datos y su posterior modificación, revelación o tráfico, provocando un perjuicio mayor para la víctima, por ejemplo, la posibilidad de comisión de delitos contra la propiedad industrial informática si el perjudicado es una empresa.

[38] De Urbano, Castrillo. *Op. Cit*. Pgs 8-9.
[39] Buenaventura, *Op Cit*. Pg. 15

En relación con la violencia descrita, es un elemento del tipo la existencia de medidas de seguridad en el sistema, por lo que resulta atípico el acceso a sistemas no protegidos[40]. Es ahí donde reside la diferencia entre el artículo 197 y el 197 bis, pues el primero no requiere la vulneración de medidas de seguridad, y el segundo sí, lo cual se debe a la necesidad de realizar las conductas de hacking e intervención de comunicaciones con un dolo específico.

El término "interceptar" engloba la observación de la comunicación y la captura y grabación de los datos, lo cual precisa instrumentos o artificios técnicos, es decir, la utilización de un dispositivo conectado a internet en nuestro caso, y por último que se realice sin consentimiento (trasmisiones no públicas[41]).

Al ser un delito de nueva impronta, carecemos de jurisprudencia relevante, pues la mayoría de las sentencias que pueden encontrarse en relación con este ilícito se cometen en el seno de un procedimiento de investigación policial sobre sospechosos, estando justificados.

Capítulo 6.- Delitos contra el honor

Cuando hablamos de delitos contra el honor, nos referimos a la injuria y a la calumnia. El Código Penal recoge los delitos contra el honor en el Título XI.
La calumnia se define en el art. 205 como "la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad". Un ejemplo sería, imputar a una persona de buena reputación y conocida defraudaciones a Hacienda o haber matado a alguien, sabiendo de antemano que es falso. La pena prevista en el art. 206 para el delito de calumnias es de "prisión de seis meses a dos años o multa de doce a 24 meses, si se propagaran con publicidad; en otro caso, con multa de seis a 12 meses". No obstante, si la acusación es cierta y consigue probarse, se eximirá de la pena al acusado. Como establece el precepto, la publicidad es lo relevante a la hora de incluir este delito entre los cometidos mediante Internet.
Por otra parte, la injuria se recoge en el art. 208 como "la acción o expresión que lesiona la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación". "Las injurias que consistan en la imputación de hechos no se considerarán graves, salvo cuando se hayan llevado a cabo con conocimiento de su falsedad o temerario desprecio hacia la verdad". También constituye injuria el insulto, siempre que se considere como grave, lo cual deberá determinarse por el juez, caso por caso, pues en algunas sentencias, las mismas expresiones han sido calificadas como graves o leves, atendiendo a las circunstancias del caso[42].

[40] Valdés-Solís: "Los delitos contra los sistemas informáticos: arts. 197 bis y 197 ter del Código Penal". Fiscalía del Principado de Asturias. 2017. Pg. 12
[41] Las describe Velasco Núñez como emisiones o transmisiones entre sistemas, diálogos entre máquinas, cuyos rastros y datos pueden dar información sobre costumbres privadas de un usuario, por ejemplo, si hay conexión con un router o si se está con un aparato encendido, que pueden dar información locativa o temporal sobre las costumbres de una persona. Velasco Núnez: "Los delitos informáticos". *Cuadernos Digitales de Formación* Nº 33. 2015, Consejo General del Poder Judicial, pág. 23.
[42] García García: *Las injurias en Internet* (máster universitario de acceso a la abogacía; trabajo de fin de máster). Universidad de Alcalá de Henares. 13 de enero de 2016. Pg. 14.

En esencia, injuriar a una persona consiste en deshonrarla o desacreditarla en público, por ejemplo, atribuir a una persona conocida y de buena reputación, un vicio importante y socialmente no aceptado perjudicándole, o atribuir a una mujer casada relaciones adulterinas, si bien dicha injuria, debe ser realizada mediante Internet, en consonancia con el resto de los delitos de este trabajo.

Tanto en injuria como en calumnias, el bien jurídico protegido es el honor y la dignidad (fama y propia estimación del ofendido), y se configuran como delitos de resultado, pues así defiende Muñoz Conde[43], exigiendo para la consumación del delito "que las injurias o calumnias lleguen a conocimiento del ofendido o de terceras personas, permitiendo calificar así también las formas imperfectas de ejecución, como la tentativa (cuando la injuria no llega a su destinatario o no se llega a publicar en la web por fallos del sistema)".

La pregunta ahora es ¿dónde deben volcarse las injurias y calumnias en Internet para que alcancen la relevancia suficiente como para constituir delito? El lugar más frecuente de proliferación de estos delitos es mediante una publicación de contenidos en páginas personales, fotografías o aportaciones a fotos, correos, comentarios en redes sociales, etc[44].

El art. 211 CP, que se refiere a disposiciones generales en los delitos contra el honor, expone y tipifica que la injuria se reputará hecha con publicidad cuando se realice a través de la imprenta, radiodifusión o cualquier otro medio de eficacia semejante. Se considera, pues, a Internet como "medio de eficacia semejante", causando un desvalor mayor a la acción. En estos casos la indemnización incluirá también los daños morales.

En Twitter, los tipos de delitos están más relacionados con comentarios políticos, o con la creación de perfiles para difundir falsas noticias o insultar. Y en Facebook, los casos más comunes son amenazas entre exparejas, insultos o la publicación de datos personales como venganza. El problema aquí reside en la libertad de expresión, y su colisión a través de las redes sociales con el derecho al honor de terceras personas, si bien ese ya es un tema constitucional que se excede de los límites de nuestro estudio.

[43] Muñoz Conde: *Derecho Penal, parte especial*. 9º Edición 2015, Tirant lo Blanch Pgs. 137 Y 138.
[44] García García, *Op. Cit*. Pg. 49

Capítulo 7.- Delitos contra la libertad

Con la reciente creación de las TICs, y su proliferación en todos los ámbitos de la vida diaria, se mejora la comunicación y las relaciones personales, pero igualmente, se incurre en riesgos de su inadecuado uso y de su abuso, pues pueden ser utilizadas para lesionar bienes jurídicos de modo intencionado. Redes sociales, chats, páginas webs y blogs entro otros, son los lugares donde se cometen los delitos contra la libertad en Internet, tales como amenazas, coacciones, acoso, o delitos contra la indemnidad sexual.

7.1.- Delitos de amenazas y coacciones

Los delitos de amenazas y coacciones se encuentran regulados en los arts. 169 a 172 del Código Penal, incluidos ambos en el título VI, relativo a los delitos contra la libertad.

El art. 169 establece:

> "El que amenazare a otro con causarle a él, a su familia o a otras personas con las que esté íntimamente vinculado un mal que constituya delitos de homicidio, lesiones, aborto, contra la libertad, torturas y contra la integridad moral, la libertad sexual, la intimidad, el honor, el patrimonio y el orden socioeconómico, será castigado."

La amenaza consiste en anunciar a una persona con causarle un mal. Si bien, el mismo artículo establece "la pena de prisión de uno a cinco años, si se hubiere hecho la amenaza exigiendo una cantidad o imponiendo cualquier otra condición, aunque no sea ilícita, y el culpable hubiere conseguido su propósito", e igualmente tipifica que "las penas señaladas en el párrafo anterior se impondrán en su mitad superior si las amenazas se hicieren por escrito, por teléfono o por cualquier medio de comunicación o de reproducción". Es aquí cuando debemos analizar la idoneidad del medio de comunicación a través del cual se realiza la amenaza, pues en el contexto de este trabajo, será Internet.

En cuanto a la amenaza que puede realizarse mediante Internet, pueden incluirse las amenazas de causar un mal que constituya delito (169), o que no lo constituya (171), de revelar secretos de otro (171.2), o de revelar la comisión de un delito (171.3), así como amenazar levemente a su pareja (171.4).

Dependiendo de la gravedad de las amenazas, y de si se realizan contra un grupo étnico o religioso podría constituir también delito de odio[45] por el artículo 510 CP. En muchas ocasiones, los delitos de amenazas van acompañados de coacciones e injurias como insultos, debiendo aplicarse así un concurso de normas.

Especial relevancia tiene el artículo 171.2 que alude al "chantaje" del siguiente modo:

> "Si alguien exigiere de otro una cantidad o recompensa bajo la amenaza de revelar o difundir hechos referentes a su vida privada o relaciones familiares que no sean públicamente conocidos y puedan afectar a su fama, crédito o interés, será castigado con la pena de prisión de dos a

[45] Moisés Barrio: "Hacking, cracking, grooming y otras conductas ilícitas en internet en el Código Penal español". *La ley penal*, nº 121. Editorial La Ley, 2016.

> cuatro años, si ha conseguido la entrega de todo o parte de lo exigido, y con la de cuatro meses a dos años, si no lo consiguiere."

El precepto divide así la posibilidad de cometer el delito sometido a condición o no, imponiendo penas mayores en el primer caso. Como vemos, se trata de un delito común, pues puede realizarse por cualquier persona con acceso a Internet o una red social, pudiendo hacer uso incluso del anonimato para escudarse. Se configura como un delito de peligro, no siendo por tanto necesario que llegue a consumarse, pues el articulado establece penas distintas y superiores en caso de que el delito se conculque o no.

El bien jurídico protegido por este delito es la libertad y la seguridad del individuo[46], tiene su mayor exponente en el artículo 17 de la Constitución Española, que dispone "toda persona tiene derecho a la libertad y a la seguridad".

Por su parte, el artículo 172 CP trata las coacciones del siguiente modo:

> "El que, sin estar legítimamente autorizado, impidiere a otro con violencia hacer lo que la ley no prohíbe, o le compeliere a efectuar lo que no quiere, sea justo o injusto, será castigado con la pena de prisión de seis meses a tres años o con multa de 12 a 24 meses, según la gravedad de la coacción o de los medios empleados."

Al igual que en las amenazas, el delito de coacciones trata de proteger el bien jurídico de la libertad tanto en el momento de la toma de decisiones, como en el de su ejercicio.

La coacción exige violencia, si bien en estos casos, lo complejo es determinar si su extensión en la intimidación producida a través de correos electrónicos y de la amenaza de publicar contenidos íntimos en Internet es equiparable a la fuerza. En opinión de Miró Llinares, "solo cuando la intimidación ejercida a través del ciberespacio sea tan grave como para ser considerada una vis compulsiva impeditiva, podrá entenderse la misma equivalente a la fuerza exigida para la violencia en las coacciones. En el resto de los casos estaremos, más bien, ante amenazas condicionales que, en muchos casos, también serán agravadas si se acaba cumpliendo la condición exigida".

Especial transcendencia tiene hoy en día, el delito de "Stalking", el cual fue introducido con la reforma del Código Penal del 2015 en el artículo 172.ter, el cual establece:

> "Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana"

El precepto tipifica una conducta que, si bien es constitutiva de acoso, y la cual trataremos a continuación en mayor profundidad, se encuentra dentro del capítulo de coacciones, pues el bien jurídico que coarta es la propia libertad de actuar de la víctima.

El artículo establece como elementos del tipo el hecho de acosar a una persona realizando una conducta de modo insistente y reiterada, por lo que no será suficiente la actuación puntual. En cuanto a las conductas típicas el precepto incluye "vigilar, perseguir a una persona a través de una red social o intentar establecer contacto reiteradamente, así como mediante el uso indebido

de sus datos personales, adquirir productos o contratar servicios, y atentar contra la libertad de esta o su patrimonio".

7.2.- Delito de ciberacoso

Cabe definir el ciberacoso como "la amenaza, hostigamiento, humillación o molestia que una persona o grupo ejerce sobre otra, haciendo uso para ello de tecnologías tales como el correo electrónico, los chats, páginas web, blogs, telefonía móvil, cámaras digitales, o videoconsolas y similares"[47] .

7.2.a).- Ciberacoso no sexual

El objetivo principal del autor de estos actos es coartar la libertad de una persona, humillarla o vejarla, de un modo repetido y sistemático, para excluirla socialmente. Si bien este tipo de actos pueden realizarse por cualquier individuo, en la gran mayoría de los casos, ocurren en entornos de menores de edad, a través de redes sociales, de modo que la doctrina ha empezado a nombrarlos como "cyberbullying", "cyberstalking", o "happy slapping"[48], si bien los dos últimos son variedades del primero.

El cyberbullying alude al acoso moral entre jóvenes, el tradicional acoso escolar, si bien este tiene lugar empleando las TIC. Se trata de un comportamiento agresivo, dañino y repetido, que es realizado en una relación interpersonal caracterizada por un desequilibrio de fuerza o poder. Como ejemplos pueden citarse enviar mensajes ofensivos a diario a la víctima, ya sean a través de chats o correos electrónicos; crear un perfil falso en una red social suplantando la personalidad de la víctima, y colgar fotos o videos con atención de desprestigiarla, etc.

De entre los ejemplos comentados, el hecho de grabar una agresión y hostigamiento físicos para posteriormente difundirla por una red social para jactarse recibe el nombre de "happy slapping"[49] (golpeando felizmente).

Por otro lado, llamar repetidamente por teléfono, enviar emails amenazadores, el seguimiento e investigación constante de información sobre una persona se denomina "cyberstalking". Dado que ya hemos analizado el delito de stakling en el artículo 172.ter, aquí se aplican aquellos casos que no pueden incluirse ni en las amenazas ni en las coacciones, se trata de aquellos supuestos en los que sin llegar a producirse necesariamente el anuncio explícito de la intención de causar algún mal (amenazas) o el empleo directo de violencia para coartar la libertad de la víctima (coacciones), se producen conductas reiteradas por medio de las cuales se menoscaba gravemente la libertad y sentimiento de seguridad de la persona[50].

[47] Buenaventura Ferrer Pujol: "Las nuevas tecnologías: injerencias en el ámbito de la privacidad. Su persecución penal". *Cuadernos digitales de formación*, nº43, 2010. Pg. 23

[48] Cuerda Arnau : "Menores y redes sociales: protección penal de los menores en el entorno digital". *Cuadernos digitales de formación*. nº30, 2013. Pgs. 13-14

[49] Guardiola: "Menores y nuevas tecnologías: los nuevos retos en el sector legal en España". *La Ley derecho de familia*, nº14, 2017. Pg. 3 y ss.

[50] Tardón Olmos, "La violencia de género a través de las nuevas tecnologías". Presidenta de la sección 27ª de la Audiencia Provincial de Madrid. Consejo General del Poder Judicial. Pg. 6

Tales conductas ofenden aspectos esenciales de la personalidad, como el derecho a la dignidad, la propia imagen, honor, intimidad, secreto de las comunicaciones, si bien el bien jurídico principal que se ve afectado con estos actos es la libertad, así como la integridad moral, y el libre desarrollo de la personalidad.

El problema reside en que llamar a alguien por teléfono, enviar cartas, emails, hacer regalos, esperarle a la salida del trabajo, como tales son actos que no revisten de implicación penal, por lo que va a ser necesaria una oposición por parte de la víctima, así como una repetición y continuidad de los actos en el tiempo, si bien el código no nos dice durante cuánto tiempo, algunos reputados especialistas han fijado como guía orientativa un periodo no inferior a un mes, si bien otros hablan de seis meses[51].

El Código Penal por su parte, utiliza un doble sistema, por un lado, el legislador va a tomar como criterio la afectación real de un bien jurídico a través de una forma de delito clásico ya tipificado, trasladado a la red. De este modo, un mismo acto de acoso puede llegar a ser constitutivo de varios delitos, como son los siguientes[52]:

-Lesiones (arts. 147 y ss CP)

- Amenazas (arts. 169 a 171 CP)

- Coacciones (art. 172 CP)

- Injurias (art. 205 y 207 CP)

- Calumnias (art. 208 y 210 CP)

- Agresiones y abusos sexuales (arts. 178 y ss CP), o embaucamiento con fines sexuales, a menores de 16 años (art. 183 ter CP)

- Homicidio doloso (art. 138 CP), homicidio imprudente (art. 142 CP) o, incluso asesinato (art. art. 138 CP).

Por último, pero más importante, la LO 1/2015 introduce, además, el nuevo delito de acoso (art. 172. Ter CP) entendiendo como tal aquellas conductas que se realicen de forma insistente y reiterada por medio de las cuales se menoscaba gravemente la libertad y el sentimiento de seguridad de la víctima, a la que se somete por ello a vigilancia, persecuciones u otros actos de hostigamiento.

El nuevo delito de acoso exige que la conducta del acosador se concrete en una de las siguientes:

> "1. La vigile, la persiga.
>
> 2. Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación.
>
> 3. Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios.

[51] Tardón Olmos, Op Cit. Pg. 10.

[52] Realiza esta clasificación, Esteban, A. 2016. "El acoso escolar o Bullying: regulación legal y derechos de las víctimas". 2016, Noticias Jurídicas, actualidad-acoso escolar. Consultado el 11/05/2018. http://noticias.juridicas.com/actualidad/noticias/10857-el-acoso-escolar-o-bullying:-regulacion-legal-y-derechos-de-las-victimas/

4. Atente contra su libertad o contra su patrimonio."

Como podemos observar, el articulado puede aplicarse indistintamente en los casos en que la víctima sea la pareja o un menor, es decir, estos delitos son genéricos, si bien dado el carácter más infantil del cyberbullying, suele realizarse en entornos de menores a través de redes sociales, siendo por el contrario el cyberstalking más utilizado entre adultos, y en concreto, con especial relevancia para los casos de violencia de género online, como veremos.

7.2.b).- Ciberacoso sexual

El ciberacoso sexual es la variante del ciberacoso que consiste en un abuso sexual virtual. Como conductas más relevantes de este delito vamos a analizar el "sexting" y el "grooming".

El ciberacoso sexual es aquella actividad de chantaje y hostigamiento a través de fotografías, videos o mensajes eróticos, en los que aparece la víctima acosada, a través de Internet. El objetivo del agresor es cometer un abuso sexual, la extorsión económica o bien la explotación pornográfica del material. El ciberacoso sexual puede dilatarse en el tiempo o puede realizarse de forma puntual; puede ejercerse por un desconocido o por una persona conocida.

La víctima de este tipo de delitos puede ser cualquier persona, hombres, mujeres y niños igualmente, si bien si la conducta se realiza con menores se denomina "child grooming", pues es un tipo de pederastia a través de las nuevas tecnologías.

"Sexting"

El sexting , acrónimo o contracción de los términos "sex" (sexo) y texting (texto, mensaje) se produce generalmente en los supuestos de ruptura de la relación de pareja, y consiste en el envío, a través de internet (WhatsApp y redes sociales) de material privado, como fotografías o videos de contenido erótico efectuados en el ámbito de la intimidad y confianza que proporciona la relación, a una lista de contactos de conocidos que, en la dinámica de transmisión viral de la información propia de las redes sociales puede multiplicarse exponencialmente, distribuyendo tales contenidos a un ilimitado número de destinatarios[53].

Los riesgos que ocasiona este tipo de delitos son entre otros, pérdida de credibilidad, vulneración de la dignidad, estigmatización y limitación del desarrollo de la libre personalidad.

Con la reforma operada por la LO 2/2015 por la que se modifica el CP, se introduce esta nueva figura como delito, tipificándolo en el art. 197.7 de dicho cuerpo legal.

> "Será castigado (…) el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona." (…)
>
> "La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa."

[53] Tardón Olmos, Op Cit. Pg.14

Como vemos, el artículo cita los actos de difundir, revelar o ceder a terceros el material sensible, y aunque el código lo incluye dentro de los delitos relativos a la intimidad, en concreto, en el capítulo del descubrimiento y revelación de secretos, en mi opinión lo trato en lo referente a delitos contra la libertad, pues considero que si bien lo que está produciendo con esta actuación es una lesión de la intimidad, el delito de sexting es una antesala a la revelación, es una extorsión, y por tanto un tipo de coacción.

"Child grooming"

Por otra parte, pero también incluido en los delitos de ciberacoso sexual, está el "child grooming", cuyo término se refiere a las acciones realizadas deliberadamente con el fin de establecer una relación y un control emocional sobre un niño o niña con la intención de preparar el terreno para un posterior abuso sexual del menor[54].

La traducción literal de la conducta significa engatusar, pues el delincuente realiza todo un proceso[55] que puede durar semanas o incluso meses, en el que primero el adulto ingresa en chats públicos con nicks que atraen a la víctima y procede a entablar lazos emocionales con él, simulando ser otro niño/a, obteniendo así datos personales y de contacto del menor. Utilizando técnicas de seducción y enviando imágenes de contenido pornográfico consigue que el menor se desnude delante de la webcam, momento en el que el delincuente ya tiene engatusada a su víctima, y le obliga a mandarle más fotos o realizar encuentros, bajo la amenaza de divulgar lo que ya tiene.
El proyecto de Ley de reforma del Código Penal de 2010 introdujo la figura del grooming en el art. 183 ter del CP, con el requisito de que la edad del menor fuera inferior a los 13 años. Posteriormente, la Ley 1 /2015 por la que se modifica el CP, ha elevado dicha edad a 16 años, ampliando así el ámbito de protección de la víctima, pues entiende que esas edades son vitales para el desarrollo de la personalidad, y que en ese momento el menor no tiene edad para consentir relaciones sexuales[56].

> "Artículo 183 ter.
>
> 1. El que a través de internet, del teléfono o de cualquier otra tecnología contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses.
>
> 2. El que a través de internet, del teléfono o de cualquier otra tecnología contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años."

[54] Berdugo Gómez de la Torre: "La reforma 5/2010 y los delitos contra la libertad e indemnidad sexual. Ciberacoso sexual- Análisis jurisprudencial". *Cuadernos digitales de formación*, Nº 40, 2012. Pg. 24.
[55] Más detalladamente, Vid. Ramos Vázquez: "El nuevo delito de ciberacoso…", cit., p. 2 y MAGRO SERVER: "El grooming o ciberacoso infantil, el nuevo artículo 183 bis del Código Penal", Revista Jurídica La Ley, núm. 7492, 2010, Pgs. 10 y ss.
[56] Pérez Vallejo: *Bullying, ciberbullying y acoso con elementos sexuales: desde la prevención a la reparación del daño.* Madrid. Dykinson S.L. 2016. Pg. 125 y ss.

El bien jurídico protegido por el tipo penal va a ser para la mayoría de la doctrina la indemnidad sexual del menor, si bien también entra en contacto con otros bienes como la intimidad, la dignidad, y la integridad moral.

En cuanto a los sujetos, de la redacción del precepto se infiere que esta modalidad delictiva puede ser realizada por cualquier persona, por lo que nos encontramos ante un delito común, donde no se exige ninguna cualificación especial.

Nos referimos así a un delito de peligro in abstracto, el legislador adelanta la barrera punitiva configurando el tipo no atendiendo a la lesión efectiva del bien jurídico protegido, sino a un comportamiento peligroso, bastando el ofrecimiento a un menor para que le mande fotografías pornográficas, así como el chantaje al mismo para que realicen un encuentro bajo la amenaza de divulgar las fotos obtenidas.

Se trata por tanto de un acto preparatorio de un delito contra la indemnidad sexual del menor, ya que su núcleo lo integran conductas dolosas tendentes a facilitar el posterior encuentro. La única novedad es que lo que antes se realizaba en parques y sirviéndose de golosinas, ahora se realiza mediante las TIC[57], cuyo potencial amplificador del peligro es lo que, de algún modo, explica que se le dé un tratamiento singular.

Problemática probatoria:

Los delitos contra la intimidad, así como contra la libertad, presentan la dificultad probatoria de las conductas delictivas, pues en este tipo de actos cometidos a través de las nuevas tecnologías, el servidor a través del que se efectúa la comunicación, la empresa prestadora del servicio (Facebook) no se encuentra en España, sino en EEUU. Junto con ello hay que añadir la volatilidad y facilidad de alteración de las pruebas por los particulares.

7.3.- Delitos de pornografía infantil

Respecto al concepto de pornografía infantil, en 1989 el Consejo de Europa la definió como "cualquier material auditivo en el que se emplee a un menor en un contexto sexual"[58]. Según Berdugo Gómez de la Torre, por "elaboración de material pornográfico" podemos entender "tanto fotografías como videos, como cualquier soporte magnético que incorpore a un menor en una conducta sexual explícita, entendiendo por ésta el acceso carnal en todas sus modalidades, la masturbación, zoofilia, o las prácticas sadomasoquistas, pero no los simples desnudos" [59]. Hoy, el Código Penal define la pornografía infantil en el párrafo segundo, del apartado b) del artículo 189.1 CP incluyendo "todo material que represente de manera visual a un menor o una persona con discapacidad necesitada de especial protección participando en una conducta sexualmente explícita, real o simulada; toda representación de sus órganos sexuales".

[57] Cuerda Arnau *Op. Cit*. Pg. 15
[58] Recomendación N° R (91)11 del Comité de Ministros del Consejo de Europa a los Estados miembros sobre la explotación sexual, la pornografía, la prostitución y la trata de niños y jóvenes mayores de edad.
[59] Berdugo Gómez de la Torre: "La reforma 5/2010 y los delitos contra la libertad e indemnidad sexual, ciberacoso sexual, análisis jurisprudencial". Cuadernos digitales de formación, Nº 40, 2012. Pg. 35.

Por tanto, la pornografía infantil debe integrarse en representaciones visuales, no siendo suficiente el material de audio ni el escrito, en el que se incluya a un menor de edad, o persona con discapacidad, realizando actos sexuales, participando de ellos o se representen sus órganos sexuales.

Por su parte, el apartado d) hace referencia a "imágenes realistas", lo cual es propio de la pornografía digital (La pornografía virtual o artificial es aquella generada íntegramente en el ordenador). La "pseudo pornografía"[60], por último, es aquella en que se insertan las voces, fotogramas o imágenes de menores reales identificables, en contextos pornográficos.

En cuanto a las conductas típicas, es decir, a los actos punibles, el artículo 189.1 contiene dos tipos de actos esencialmente típicos:

> "1. Será castigado con la pena de prisión de uno a cinco años:
>
> a) El que captare o utilizare a menores de edad o a personas con discapacidad en espectáculos exhibicionistas o pornográficos, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte (…).
>
> b) El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de pornografía infantil."

El legislador penaliza dos modalidades de delito, por un lado, la captación o utilización del menor o discapacitado para pornografía, y por otro, la producción y distribución del material ilícito. Se trata por tanto de un delito de acción y de mera actividad, de carácter esencialmente doloso, del que puede ser autor cualquier persona, pero del que solamente puede ser sujeto pasivo el menor o discapacitado.

El delito de pornografía infantil, tipificado como advertimos en el art. 189, se encuentra enmarcado en el capítulo referente a los abusos y agresiones sexuales a menores de dieciséis años, que a su vez está incluido en el título VIII, relativo a la libertad e indemnidad sexuales, por lo tanto el bien jurídico protegido será la indemnidad sexual en el propio acto, si bien en la conducta de la distribución lo que se está afectando es a la propia dignidad del menor, junto al desarrollo de su libre personalidad.

Analizando este delito desde la órbita de la comisión de delitos a través de Internet, cuyo tratamiento es el que nos interesa, dejamos aparte el acto originario de la utilización del menor o discapacitado para la producción del material pornográfico, lo cual se realiza en el plano físico sin entrar en la Red necesariamente, y nos centraremos en la distribución del mismo vía Internet.

La difusión de pornografía infantil hace referencia al acto de compartir archivos mediante la utilización en Internet de un programa de los denominados P2P[61] (emule, Torrent, Jdowndloader), siendo así subsumible en el art. 189.1.b) cuando pueda acreditarse dolo en la difusión. En las redes P2P al tiempo que se descargan archivos ajenos, se permite a terceros la

[60] Tanto la pornografía infantil, pornografía técnica, virtual o pseudo pornografía están tratados ampliamente en la Circular 2/2015, de 19 de junio de 2015, de la Fiscalía General del Estado, sobre los delitos de pornografía infantil tras la reforma operada por LO 1/2015. La Ley Digital 360, La Ley 147/2015.
[61] Pérez González: "Protección penal de la propiedad intelectual en entornos P2P y riesgo de ofuscamiento de la norma". *Revista electrónica de ciencias criminológicas*, nº3. 2018. Pg. 18.

descarga de archivos propios, creando una carpeta de intercambio[62]. Se imputa así al usuario que permitió el acceso a su ordenador desde la pública de la red, a través de uno de estos programas, compartiendo archivos que contengan este tipo de pornografía. El sujeto no servía material pornográfico a los destinatarios, pero permite que otros accedan al mismo poniéndolo, por tanto, a disposición de terceros. No obstante, el Tribunal Supremo[63] ha matizado, que estos casos deben analizarse individualmente según sus características, material y conocimiento del autor.

Junto con la difusión y la posesión de estos contenidos, la reforma 1/2015 incluyó el "acceso a sabiendas a pornografía infantil", en el art. 189.5:

> "El que para su propio uso adquiera o posea pornografía infantil (…), será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años.
>
> La misma pena se impondrá a quien acceda a sabiendas a pornografía infantil (…) por medio de las tecnologías de la información y la comunicación."

No obstante, este tipo de acceso a sabiendas plantea graves dificultades probatorias, así como la exigencia de un dolo directo, el cual no siempre puede demostrarse dada la gran cantidad de publicidad pornográfica en la red, dando posibilidad a un acceso involuntario o por accidente.

Por otro lado, se incluyen como supuestos agravados también la violencia física o sexual sobre los menores, la puesta en peligro de su vida o salud, así como la notoria importancia del material pornográfico o la pertenencia del culpable a una organización o asociación. Junto con estos, está especialmente penado el caso de que los hechos sean cometidos por el ascendiente, tutor, curador o maestro del menor, y la reincidencia.

Capítulo 8.- Delitos contra el patrimonio y orden socioeconómico

8.1.- Delito de daños informáticos

El delito de daños informáticos se encuentra regulado en el art. 264 CP:

> "El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años."

El precepto hace referencia a varias conductas para evitar el vacío normativo, las cuales deben entenderse como: "borrar" en el sentido de destruir los datos, formateando el soporte o destruyéndolo directamente, siendo irrelevante que puedan volver a recuperarse mediante un back-up; "deteriorar" por su parte, hace referencia a menoscabar la integridad del contenido

[62] Berdugo Gómez de la Torre. Op. Cit. Pg. 38.
[63] Circular 2/2015, *Op.Cit*. Pg.9.

informático y "suprimir" a impedir al titular de los datos acceder de manera permanente o temporal a dichos datos (ocultación). Por último, "hacer inaccesibles" abarca la acción de obstaculizar la disponibilidad y la correcta utilización de los datos informáticos[64].

Si bien el precepto requiere que "el resultado producido sea grave", no aporta un criterio para identificar la gravedad del daño, por lo que será labor de los jueces determinarlo conforme a criterios objetivos.

Con la reforma de 2015 el legislador añade más supuestos agravantes, entre ellos, "pertenencia a organización criminal; ocasionar daños de especial gravedad o afectar a un número elevado de sistemas informáticos; perjudicar gravemente el funcionamiento de servicios públicos esenciales; crear una situación de peligro grave para la seguridad del Estado; utilización de medios del art. 264.ter".

Como hemos dicho anteriormente en los delitos contra la intimidad, los hackers no producen daños, sino que más bien fisgonean, sin embargo, en el campo de los delitos contra el patrimonio, encontramos conductas como las siguientes[65]:

Crackers: invasores de programas informáticos ajenos; crack significa romper en inglés, realizan acciones dañinas, desde un test del borrado de información al robo de la misma con el único objetivo de venderla al mejor postor, normalmente la competencia.

Ciberpunk: vándalos electrónicos, buscan el daño por el daño, siendo los virus y las bombas lógicas sus manifestaciones más frecuentes. (son una vertiente radicalizada de los crackers)

Virus informático: programa elaborado accidental o intencionadamente, que se introduce y se transmite a través de la red telefónica de comunicación entre ordenadores causando diversos tipos de daños a los sistemas. Los virus pueden ser creados por los Ciberpunkers o por los Viruckers**.** Uno de los mayores problemas que causan los virus es el daño directo y el lucro cesante, no hay nada que hacer salvo prevención, especialmente *"El caballo de Troya, o el Worm.* Por otra parte también se producen acciones como "el caballo de Troya", "la estafa e datos", "trampas y bombas lógicas" etc.

Como vemos, el delito de daños se configura como un delito de resultado, pues provoca graves daños informáticos en relación con datos, utilizando como vehículo de difusión Internet. En cuanto a los sujetos activos, claramente se requerirá de cierta formación o conocimientos técnicos para saber desarrollar un virus informático y difundirlo por la red, así como para acceder y borrar datos de servidores ajenos, si bien sujeto pasivo puede ser cualquier individuo o persona jurídica (contra quienes suelen realizarse mayoritariamente).

Al igual que en los delitos contra la intimidad, se protege el bien jurídico de la seguridad de los sistemas informáticos, si bien dado el plus de antijuridicidad, es decir, dado el daño producido, también se protege el patrimonio informático.

Por otro lado, el 264.3 castiga a quien de manera agravada dañe a "intereses generales", por ej. el tráfico aéreo, naval o ferroviario, estructuras hospitalarias, centros nucleares, etc.

[64] Salvadori : "Los delitos informáticos introducidos en el Código Penal español con la Ley Orgánica 5/2010. Perspectiva de derecho comparado". Universidad de Verona-Barcelona. ADPCP, Vol. LXIV, 2011. Pg. 238.
[65] Realiza esta clasificación Pérez Machío & De la Cuesta Arzamendi en *Derecho Penal Informático*, Pamplona, Civitas, 2013, capítulo 3.

8.2.- Delitos contra la propiedad intelectual e industrial

La protección de la propiedad intelectual por la vía penal se regula entorno a los artículos 270, 271 y 272 del Código Penal, que fueron reformados por la LO 1/2015. El art. 270 establece:

> "Será castigado (…), el que con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero, reproduzca, plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicamente, en todo o en parte, una obra o prestación literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios."

El artículo 270 establece como conductas típicas "reproducir" (fijación en un soporte de la obra protegida); "plagiar" (copia de lo sustancial de las obras ajenas, dándolas como propias[66], si bien el plagio protege un derecho moral del autor); "distribuir" (puesta a disposición de terceros de la obra[67], es decir, la venta o el cambio, por ejemplo); y "comunicar públicamente" ("la puesta a disposición del público de una obra sin tener que distribuir ejemplares, quedando fuera de la definición cuando se hace en el ámbito doméstico"[68]).

Salvo el plagio, todas las conductas pueden realizarse por Internet; se daría la conducta de reproducir si el propietario de la página web sube los archivos a la web, o una comunicación pública si están disponibles para descargarlos o poder visualizarlos por medio del "streaming". En cuanto a distribución podría considerarse las ventas que se realizan por páginas como Ebay o Wallapop de películas originales como venta de segunda mano.

Ahora bien, analizando el precepto en mayor profundidad vemos que exige "el que con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero", lo cual puede abarcar cualquier ingreso obtenido mediante esa conducta, frente a la anterior redacción que decía "de cualquier otro modo explotar económicamente", pues con ella numerosos casos se escapaban por no apreciarse una explotación económica en la venta de varios dvds, si bien con la reforma se permite la inclusión de todos los casos posibles.

En cuanto a lo que se representa, distribuye o comunica, el precepto establece que debe ser una obra o prestación literaria, artística o científica, lo cual amplía el art. 10 LPI incluyendo "libros, folletos, composiciones musicales, obras dramáticas, cinematográficas o teatrales, fotografías, programas de ordenador, etc".

Por lo tanto, el bien jurídico protegido por este delito será la propiedad intelectual, es decir, el patrimonio personal de los individuos. Al igual que en los delitos de daños, puede ser sujeto activo cualquier persona con los conocimientos técnicos para llevarlo a cabo, y puede ser sujeto pasivo cualquier persona física o jurídica de la que puedan privar de una obra literaria, artística o científica. Por supuesto la conducta debe llevarse a cabo sin la correspondiente autorización de los titulares de los derechos que se están vulnerando, y con dolo directo, si bien en ciertos casos se acepta el dolo eventual.

---

[66] Plagio. (2017). En: Diccionario de la Lengua Española, 23rd ed. [online] Madrid.

[67] Art. 19 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

[68] Art. 20 LPI. *Op. Cit*.

El apartado segundo del artículo 270 establece una conducta distinta de las anteriores, el "facilitar de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual". Este precepto está dirigido a las webs de enlaces, las cuales no alojan directamente ningún contenido protegido, sino que proporcionan los enlaces que permiten acceder a los mismos[69]. Un ejemplo serían las webs que obtienen beneficios mediante la publicidad, alojando simples enlaces a otras páginas para la verdadera descarga o visionado.

El verdadero medio a través del cual se realizan la mayoría de los delitos contra la propiedad intelectual en internet es mediante los sistemas de intercambio de archivos P2P comentados en los delitos de pornografía infantil.

El precepto también prevé en el apartado 5.c) del artículo 270, el "facilitar la realización de las conductas típicas descritas eliminando o modificando las medidas tecnológicas incorporadas en ellas". El precepto alude a los crackers que crean programas para eliminar la protección de las obras y poder realizar las conductas típicas ya comentadas.

Finalmente, el art. 271 fija una serie de agravantes específicas, en los casos en de especial transcendencia económica del beneficio obtenido; especial gravedad de los hechos, atendiendo al valor de los objetos o número de obras; así como la pertenencia del autor a una organización o asociación, o la utilización de menores de 18 años para cometer estos delitos.

Delitos contra la propiedad industrial

En España la normativa más relevante se halla en la Ley de Patentes, Ley 24/2015, de 24 de julio, la Ley 17/2001 de 7 de diciembre, de Marcas y los arts. 273 a 277 del Código Penal.

El tipo básico de este delito en relación con Internet castiga a quien:

> "con fines industriales o comerciales, sin consentimiento del titular de un derecho de propiedad registrado y con conocimiento del registro, fabrique, importe, posea, utilice, ofrezca o introduzca en el comercio objetos amparados por tales derechos".

Por tanto, el delito contra la propiedad industrial se caracteriza por realizarse sin consentimiento del titular del derecho en exclusiva, existiendo un registro, el cual es conocido por el sujeto activo, el cual vulnera el mismo con fines industriales y comerciales, es decir, para lucrarse. Estas conductas son susceptibles de realizarse en Internet, ya sea a través de la comercialización de las propias patentes digitalizadas, o a través de la venta en mercados digitales de los productos patentados sin la correspondiente autorización, no obstante, el precepto nada dice de Internet, por lo que deberemos entender esta posibilidad incluida mediante el ofrecimiento o la introducción en el comercio, concibiendo la red como un auténtico mercado.

El objeto material del delito serán tanto las patentes de invención, los modelos de utilidad, los diseños industriales y los signos distintivos por marcas y nombres comerciales. Como bien jurídico protegido por este tipo penal, se encuadra el "derecho de uso o explotación en exclusiva" de los objetos registrados en la Oficina Española de Patentes y Marcas.

[69]Miró Llinares: *Internet y delitos contra la propiedad intelectual*. Madrid. Sociedad General de Autores y Editores. 2005. Pgs.28 y ss.

Estas patentes y modelos de utilidad son invenciones y diseños que tienen valor en sí mismos, o aportan valor a un bien ya creado de antemano (como los diseños industriales), por lo que en muchos casos la víctima suele ser una persona jurídica[70].

En cuanto a los supuestos agravantes, se aplican los mismos que para los delitos de propiedad intelectual.

Los delitos referentes a propiedad intelectual e industrial se caracterizan por ser delitos de mera actividad, el tipo se consuma con la mera realización de la conducta típica descrita en el tipo, si bien en los delitos contra la propiedad industrial se exige un plus de antijuridicidad, un dolo directo, es decir, un conocimiento de que el derecho que se está vulnerando se encuentra registrado y protegido legalmente de antemano.

8.3.- Delitos de estafas informáticas (ciberfraude)

Como ya hemos dicho anteriormente, Internet se configura como un verdadero mercado internacional, un lugar en el que desarrollar actividades comerciales tanto empresas como particulares, posibilitando las relaciones de intercambio a través de distintas webs y aplicaciones de venta de segunda mano. Sin embargo, siempre existe la posibilidad de caer en los riesgos del ciberfraude.

Como dice Miró Llinares, hablamos de ciberfraude para denominar a "toda una variedad de conductas en las cuales las redes telemáticas se convierten en instrumento esencial mediante el cual lograr un beneficio patrimonial ilícito derivado de un perjuicio patrimonial a una víctima"[71].

Algunos de los más conocidos son las estafas de inversión, las estafas piramidales realizadas a través de Internet, las ventas online defraudatorias en las que no se envía el producto comprado o no se paga el recibido o se cobran servicios no establecidos previamente, etc.

El artículo 248 del Código Penal trata de concretar cuales son las conductas en las que se ejecutan fraudes, y establece que "cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno".

El elemento esencial del delito es el engaño, el cual es definido como "hacer creer a alguien que algo falso es verdadero[72]" o "seducir a alguien con halagos y mentiras".

Ahora bien, dicho engaño debe ser "bastante" para la consecución de los fines propuestos, y de suficiente entidad como para lograr un traspaso patrimonial, con el consiguiente perjuicio para el sujeto pasivo.

Dicho traspaso se produce por un error esencial en la víctima, que desconoce lo que realmente estaba contratando o adquiriendo, a consecuencia de la actuación fraudulenta y dolosa por parte del sujeto activo, el cual actúa con ánimo de lucro, es decir, con la intención de obtener un enriquecimiento patrimonial a costa de su víctima.

---

[70] Mata y Martín: "Criminalidad informática: una introducción al cibercrimen". *Revista de actualidad penal* nº 37, 2003. Pg. 12

[71] Miró Llinares: L*a respuesta penal al ciberfraude, especial atención a la responsabilidad de los muleros del phishing*. *Revista Electrónica de Ciencia Penal y Criminológica* nº CDJ15-12. 2013. Pg. 5.

[72] Engaño: (2017). En: Diccionario de la Lengua Española, 23rd ed. [online] Madrid.

El artículo 248.2 considera culpables de estafa aquellos que para obtener la disposición patrimonial ajena le engañen, manipulen informáticamente o usen algún artificio semejante como programas informáticos especialmente diseñados para la comisión de estos delitos, así como aquellos que utilicen tarjetas de crédito o débito ajenas para realizar operaciones comerciales en perjuicio de tercero.

Una de las conductas más realizadas en este ámbito es el phishing[73], o pesca de incautos, el cual emplea tanto ingeniería social, como subterfugios técnicos para robar los datos de identidad personales de los consumidores y los de sus tarjetas de crédito o cuentas bancarias. El uso de la ingeniería social se produce cuando se utiliza la identidad personal de otro (spoofing) mediante la falsificación de sitios web, para conducir a los consumidores a que confíen en la veracidad del mensaje y divulguen los datos objetivos. Suelen emplearse sms, redes sociales, correo electrónico o incluso a través de videojuegos online. Finalmente, el delincuente usa los datos de la víctima suplantando su identidad, o vendiéndola a terceros (números de tarjetas de crédito), generando así un mercado negro de compraventa de información robada[74]. Junto con el phishing, el uso de malware es otra de las conductas más utilizadas para cometer este tipo de delitos, haciendo uso de un software malicioso en el ordenador del usuario.

En cuanto a la gravedad del delito, el artículo 249 establece que si lo defraudado no excediere de 400€, será considerado como delito leve imponiéndose una pena multa de uno a tres meses, mientras que el artículo 250 fija como supuestos agravados cuando la estafa recaiga sobre cosas de primera necesidad o viviendas, se perpetre haciendo uso de la firma de otra persona, revista especial gravedad o la cantidad defraudada supere los 50.000€ o afecte a un elevado número de personas, se cometa "estafa procesal" o si el culpable al delinquir hubiera incurrido en tres delitos del mismo capítulo referente a estafas, en estos casos la pena será de prisión de uno a seis años y multa de seis a doce meses.

8.4.- Delitos de Ciberterrorismo y propaganda de grupos extremistas

El terrorismo internacional de corte yihadista se caracteriza por haber introducido entre sus métodos la captación de seguidores a través de las nuevas tecnologías, en muchos casos utilizando redes sociales, chats públicos y la red profunda. Con estos nuevos instrumentos consiguen la captación, adiestramiento y adoctrinamiento en el odio, para emplearlos contra aquellos que, en su ideario extremista y violento, sean calificados como enemigos[75].

El DLA define terrorismo[76] como "sucesión de actos de violencia ejecutados para infundir terror", o "actuación de bandas organizadas, que reiteradamente y por lo común de modo indiscriminado, pretende crear alarma social con fines políticos".

[73] De la Mata Barranco & Hernández Díaz: "Los delitos vinculados a la informática en el derecho penal español", en *Derecho penal Informático* (parte III, capítulo III). Pamplona, Civitas, 2010. Pgs. 180-185.
[74] Miró Llinares. *Op. Cit*. Pg. 9
[75] Agudo Fernández: *Terrorismo en el siglo XXI, (la respuesta penal al escenario mundial)*. Madrid, Editorial Dykinson, 2016. Pg. 119.
[76] Terrorismo. (2017). En: Diccionario de la Lengua Española, 23rd ed. [online] Madrid.

La reforma de 2015[77] introduce en el Código Penal el delito de adiestramiento dentro de los delitos de terrorismo, en el artículo 575, el cual castiga "a quien, con la finalidad de capacitarse para llevar a cabo cualquiera de los delitos tipificados en este Capítulo, reciba adoctrinamiento para facilitar la comisión de alguna de tales infracciones".

El CP adelanta la barrera punitiva al momento en el que se desarrolla una actividad tendente a la radicalización de personas, que no habiendo realizado ninguna acción terrorista, están en disposición de hacerlo precisamente a consecuencia de dicha capacitación, adoctrinamiento y formación.

De esta manera, el Código Penal castiga tanto el adoctrinamiento de terceras personas, como el auto adoctrinamiento, si bien en el contexto que nos interesa es a través de Internet, pues dicho resultado puede conculcarse mediante visitas constantes a páginas webs de riesgo por el propio individuo, o por el contacto virtual con terceras personas, miembros de organizaciones criminales, que utilicen esos chats para captar nuevos miembros.

El art. 577 castiga al adiestrador –"el que lleve a cabo, recabe o facilite cualquier acto de colaboración con las actividades o las finalidades de una organización, grupo o elemento terrorista, o para cometer cualquiera de los delitos comprendidos en este Capítulo"- y el art. 575.2 penaliza el auto adiestramiento –"a quien, con la misma finalidad de capacitarse para cometer alguno de los delitos tipificados en este Capítulo, lleve a cabo por sí mismo cualquiera de las actividades previstas en el apartado anterior"-.

Si bien el artículo que verdaderamente detalla la conducta terrorista a través de Internet es el 579.1:

> "Será castigado (…) el que, por cualquier medio, difunda públicamente mensajes o consignas que tengan como finalidad o que, por su contenido, sean idóneos para incitar a otros a la comisión de alguno de los delitos de este Capítulo."

La cuestión aquí sería debatir acerca de qué debe entenderse por dicha proposición adiestramiento, y si cabe incluir por ejemplo los tuits del caso de Cassandra o Strawberry, referentes a enaltecimiento del terrorismo. Si bien en los casos de los tuits simplemente se "enaltecía" el terrorismo, con frases vulgares, pero sin el propósito de adoctrinar a nadie, la captación y el adoctrinamiento consisten básicamente en lo que tipifica el artículo 575.1, "adiestramiento militar o de combate, o en técnicas de desarrollo de armas químicas o biológicas, de elaboración o preparación de sustancias o aparatos explosivos, inflamables, incendiarios o asfixiantes, o específicamente destinados a facilitar la comisión de alguna de tales infracciones".

Como elementos del tipo, la conducta debe realizarse con dolo, y el mensaje trasmitido deberá ser idóneo para la incitación. La nueva definición de la proposición para delinquir es la siguiente: "La proposición existe cuando el que ha resuelto cometer un delito invita a otra u otras personas a participar en él."[78]

[77] Barber Burusco: "Del delito de difusión o propaganda terrorista a la desmesurada expansión de la punición de actos preparatorios". *Cuadernos de Política Criminal*, Nº 116. 2015. Pgs. 39-44
[78] Barber Burusco, *Op. Cit*. Pg. 59

CONCLUSIONES

Junto con el desarrollo tecnológico, la globalización del mercado y la economía, la modificación de la informática (encriptación), la dificultad de determinación de los ámbitos espacial y temporal, y las propias debilidades de los sistemas de datos, unido al anonimato de la Red, en su doble vertiente como derecho y como riesgo, la existencia de redes wifi públicas que permiten el acceso desde sitios abiertos, y proveedores de servicios de Internet (paginas web) que no se responsabilizan de los contenidos que publicitan, generan una gran inseguridad de los usuarios al transitar por la Red, siendo la base o núcleo duro, que justifica la necesidad de creación de un corpus normativo único que aglutine todos los delitos que puedan cometerse a través de Internet.

Como principal problema, el Código Penal no cita concretamente a Internet como un medio para la comisión de los delitos que trata, sino que en muchas ocasiones utiliza expresiones de las que debe interpretarse que se recoge a la red como medio comisivo, nos referimos a artículos como el 197.bis que establece "por cualquier otro medio", o la referencia a la "publicidad" del art. 205 en los delitos relativos al honor, así como a "cualquier otro medio de eficacia semejante" del art. 211 o "por cualquier otro medio de comunicación" por el art. 169.

Junto con ello, encontramos dificultad para entender qué debe considerarse por conceptos concretos de los cuales el Código no aporta definiciones, debiendo acudir a leyes extrapenales para comprenderlos y convirtiéndose así en conceptos jurídicos indeterminados, tales como "datos reservados", conductas de "hacking o intrusismo informático", o "engaño bastante" en el art. 248 relativo a las estafas.

En cuanto a los bienes jurídicos afectados, como hemos dicho estos delitos ofenden aspectos esenciales de la personalidad, como el derecho a la dignidad, honor, intimidad, la libertad e integridad moral y patrimonio. Esta afectación a múltiples bienes jurídicos justifica que actualmente estos delitos se dispersen por todo el Código Penal, como en los delitos de acoso no sexual, en los cuales se va a tomar como criterio la afectación de un bien jurídico a través de un delito clásico y tipificado, trasladado éste a la red generando en ocasiones mayor dificultad para determinar el bien jurídico concreto, así como en los delitos contra la intimidad, en los cuales se considera la lesión de la misma como un paso previo para un delito posterior que afecte a la seguridad de las comunicaciones y sistemas informáticos.

En mi opinión, deberíamos reunir todos los posibles delitos informáticos en un único capítulo del código penal, bajo un bien jurídico general que los acumule y sirva como criterio interpretativo de los elementos típicos; dicho bien jurídico nuevo, a mi modo de ver es una suerte de "tranquilidad de deambular por Internet sin intromisiones delictivas", la posibilidad, sino el derecho de todo usuario de la red, de navegar sin el constante miedo de lo que pueda pasar si clica por error en una página, si abre un correo, o de preocuparse por si a su hijo le habla un desconocido por una red social.

Por otro lado, en relación con los delitos contra la libertad, el art. 169 sitúa la comisión por un medio de comunicación en la mitad superior de la pena, debiendo entenderse que Internet es dicho medio, y si bien este delito se sitúa como un agravante, cabe preguntarse por qué en el

resto de los delitos no, cuando de ser así, supondría una auténtica medida de lucha contra los delitos en Internet. Por otro lado, consideramos acertada la decisión del legislador de modificar la expresión del art. 270 cambiando de "ánimo de lucro" a "obtención de un beneficio económico directo o indirecto y en perjuicio de tercero", abarcando así los supuestos que anteriormente escapaban de control por su escasa transcendencia económica, lo cual nos hace preguntarnos también, que si es posible precisar tanto en algunos casos, por qué dejar otros con menor protección y claridad. Estos problemas de disonancias entre tipos delictivos se resolvería igualmente si reunimos todos los delitos informáticos en un único capítulo, aplicando unidad de criterios a la sistematización de los mismos, así como a la imposición de las penas correspondientes, pues en relación con esto último, debemos criticar la laxitud de la pena impuesta por el art. 249 en los delitos de ciberestafas, pues deja desamparados a quienes sean estafados en una cuantía menor de 400€, dejando al delincuente libertad para realizar estas conductas hasta dicha cantidad con un mínimo riesgo del pago de una pena multa.

Dicho así, si se trataran todos estos delitos en único capítulo del Código Penal, estableciendo unos criterios de actuación conjunta internacional, aportando ciertas definiciones para poder tipificar mejor las conductas delictivas y aportar mayor seguridad jurídica, estableciendo medidas de control que posibilitaran la mejor concreción del delincuente, y bajo el reconocimiento de un bien jurídico nuevo y más general, se solventarían los problemas espacio-temporales, fijando el momento y lugar de comisión, la determinación de responsabilidades sería más sencilla, pues se precisarían mejor las modalidades de autoría, y se reducirían los delitos en Internet, sintiéndose así los usuarios realmente protegidos, y los delincuentes más vigilados.

Bibliografía

- Agudo Fernández, E.: *Terrorismo en el siglo XXI, (la respuesta penal al escenario mundial)*. Madrid, Editorial Dykinson, 2016.
- Barber Burusco, S.: "Del delito de difusión o propaganda terrorista a la desmesurada expansión de la punición de actos preparatorios". *Cuadernos de Política Criminal*, Nº 116. 2015. Pgs. 33-74.
- Barroso Toledo, R.: "Los delitos en Internet: Un enfoque desde la pornografía infantil en la red". *Revista F@ro*, Nº 13, 2011. Facultad de Ciencias Sociales, Universidad de Playa Ancha, Valparaíso, Chile.
- Berdugo Gómez de la Torre, J.R.: "La reforma 5/2010 y los delitos contra la libertad e indemnidad sexual. Ciberacoso sexual- Análisis jurisprudencial". *Cuadernos digitales de formación*, Nº 40, 2012.
- Briggs, A. y Burke, P.: *De Gutenberg a Internet, una historia social de los medios de comunicación*. Madrid, Santillana Ediciones Generales, S. L., 2002. Pgs. 249-348.
- Buenaventura Ferrer Pujol, F. "Las nuevas tecnologías: injerencias en el ámbito de la privacidad. Su persecución penal". *Cuadernos digitales de formación*, nº43, 2010.
- Climent Barberá: "La justicia penal en Internet. Territorialidad y competencias penales". *Cuadernos de derecho judicial*, nº10, 2001.
- Cruz de Pablo, J.A. "Particularidades en los procesos penales por delitos contra la propiedad industrial en el mundo digital". *Cuadernos digitales de formación*, nº4, 2014.
- Cuerda Arnau M.L. "Menores y redes sociales: protección penal de los menores en el entorno digital". *Cuadernos digitales de formación*. nº30, 2013.
- De la Cuesta Arzamendi, J.L. (director) y De la Mata Barranco, N.J. (coordinador) «*Derecho penal Informático*». Pamplona, Civitas, 2010. Pgs. 15-247.
- Encinar del Pozo, M.A. "La conservación y cesión de los datos relativos a las comunicaciones electrónicas para la investigación penal: ¿una cuestión cerrada?". *Cuadernos digitales de formación*, nº43, 2016.
- Fernández de Teruelo, J.: *Cibercrimen, los delitos cometidos a través de Internet*. Constitutio Criminalis Carolina, 2007.
- Fernando Miró Llinares: "La oportunidad criminal en el ciberespacio". *Revista Electrónica de Ciencia Penal y Criminología* 2011.
- Galán Muñóz, A.: *El fraude y la estada en los sistemas informáticos*. Valencia. Tirant lo Blanch. 2005.
- García García, A. M.: *Las injurias en Internet* (máster universitario de acceso a la abogacía; trabajo de fin de máster). Universidad de Alcalá de Henares. 13 de enero de 2016.
- García Mexía, P.: *Principios de derecho en Internet*. 2ª Edición, Tirant lo Blanch, 2005.
- González Rus, J. J. *Los ilícitos en la red: Hackers, Crackers, Cyberpunks, Sniffers, denegación de servicio y otros comportamientos semejantes*. En *El Cibercrimen:*

Nuevos retos jurídico-penales, nuevas respuestas político criminales. Romeo Casabona (Coordinador) Ed. Comares, Granada. Pgs. 241-271)

- Guardiola, M.: "Menores y nuevas tecnologías: los nuevos retos en el sector legal en España". *La Ley derecho de familia*, nº14, 2017.
- Huete Nogueras, J.J. "Delincuencia informática. Encuentro de la Sala Segunda del Tribunal Supremo con jueces y magistrados del orden penal: jurisprudencia penal". *Cuadernos digitales de formación*, nº32, 2011. Incluido en el número monográfico sobre Encuentro de la Sala Segunda del Tribunal Supremo con jueces y magistrados del orden penal: jurisprudencia penal (2011) de Cuadernos Digitales de Formación 32 - 2011 (Director: Joaquín Giménez García).
- López Moreno, J. y Fernández García, E.M. "Comunicación, la World Wide Web como vehículo de la delincuencia: supuestos frecuentes". *Cuadernos de derecho judicial*. Nº. 10, 2001 (Ejemplar dedicado a: Internet y derecho penal / Juan José López Ortega), págs. 399-456.
- Magro Server, V.: "El grooming o ciberacoso infantil, el nuevo artículo 183 bis del Código Penal", Revista Jurídica La Ley, núm. 7492, 2010,
- Magro Servet, V.: "El delito de stalking o acoso en la violencia de género en la reforma del Código Penal". *Cuadernos digitales de formación*, nº56, 2016.
- Mata y Martín, R.M. "Protección penal de los derechos del autor en Internet". *Estudios de Derecho Judicial* 138/2007. Incluido en el número monográfico sobre Las últimas reformas penales de Estudios de Derecho Judicial 138 - 2007 (Director: Salvador Francisco Javier Gómez Bermúdez).
- Mata y Martín: "Criminalidad informática: una introducción al cibercrimen". *Revista de actualidad penal* nº 37, 2003.
- Miró Linares, F. "La victimización por cibercriminalidad social". *Revista española de* investigación criminológica, nº 11, artículo 5, 2013.
- Miró Llinares, F.: "Derecho Penal, Cyberbullying y otras formas de acoso (no sexual) en el ciberespacio". *Revista de Internet Derecho y Política* Nº 16. 2013. Pgs. 61-75.
- Miró Llinares, F.: "La respuesta penal al ciberfraude, especial atención a la responsabilidad de los muleros del phishing*"*. *Revista Electrónica de Ciencia Penal y Criminológica* nº 15-12. 2013.
- Miró Llinares: *Internet y delitos contra la propiedad intelectual*. Madrid. Sociedad General de Autores y Editores. 2005.
- Moisés Barrio, A.: "Hacking, cracking, grooming y otras conductas ilícitas en internet en el Código Penal español". *La ley penal*, nº 121. Editorial La Ley, 2016.
- Morón Lerma, E. *Internet y derecho penal: Hacking y otras conductas ilícitas en la Red*. Editorial Aranzadi, 2ª Edición.
- Muñoz Conde, F.: *Derecho Penal, parte especial*. 9º Edición 2015, Tirant lo Blanch.
- Pérez González, S.: "Protección penal de la propiedad intelectual en entornos P2P y riesgo de ofuscamiento de la norma". *Revista electrónica de ciencias criminológicas*, nº3. 2018.
- Pérez Vallejo, A.M.: *Bullying, ciberbullying y acoso con elementos sexuales: desde la prevención a la reparación del daño.*. Madrid. Dykinson S.L. 2016.

- Salvadori I.: “Los delitos informáticos introducidos en el Código Penal español con la Ley Orgánica 5/2010. Perspectiva de derecho comparado”. Universidad de Verona-Barcelona. ADPCP, Vol. LXIV, 2011. Pgs. 222-252.
- Terceiro, J. B.: “Evolución tecnológica” en *Socied@d Digital. Del homo sapiens al homo digitalis*. Madrid, Alianza Editorial. 1996. Pgs.14-36.
- Urbano Castrillo, E.: “Revelación informática de secretos y daños informáticos”. Cuadernos digitales de formación, nº22, 2009.
- Velasco Núnez, E.: “Los delitos informáticos”. *Cuadernos Digitales de Formación* Nº 33. 2015, Consejo General del Poder Judicial.
- Velasco Núñez, E, “Crimen organizado, Internet y nuevas tecnologías”. *Cuadernos digitales de formación*, nº42, 2010.
- Velasco Núñez, E. “Eliminación de contenidos ilícitos y clausura de páginas web en Internet (medidas de restricción de servicios)”. *Cuadernos de derecho judicial*, 2007, tomo 3.
- Velasco Núñez, E. “Medidas restrictivas en Internet: cómo retirar contenidos ilícitos”. *Cuadernos digitales de formación*. nº52, 2008.
- Velasco Núñez, E.: *Delitos cometidos a través de Internet, cuestiones procesales*. Madrid, Editorial La Ley, grupo Wolters Kluwer S.A. 2010.
- Velasco San Martín, C.: *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet*. Valencia. Editorial Titant lo Blanch. 2012.